REMARKS

The above amendments to the above-captioned application along with the following remarks are being submitted as a full and complete response to the Office Action dated July 16, 2004. In view of the above amendments and the following remarks, the Examiner is respectfully requested to give due reconsideration to this application, to indicate the allowability of the claims, and to pass this case to issue.

Status of the Claims

As outlined above, claims 1, 2, 5, 7, 9, 11 and 13 are being amended to correct formal errors and to more particularly point out and distinctly claim the subject invention. Support for the amendments may be found throughout the disclosure of the invention.

Additional Amendments

The drawings and abstract are being amended to correct formal errors and to better disclose and describe the features of the present invention as claimed. Applicant hereby submits that no new matter is being introduced into the application through the submission of this response.

Formal Objections or Rejections

Claims 1 - 13 were rejected under 35 U.S.C. §112, second paragraph, for being indefinite on the grounds that parameters in the claims were not clearly defined. Further, claims 1 – 13 were rejected under 35 U.S.C. §101 as being directed to non-statutory subject matter. As set forth above, the claims are being amended in accordance with the Examiner's requirements, thereby rendering moot the above-noted formal rejections.

Prior Art Rejections

Claims 1, 5 and 9 were rejected under 35 U.S.C. § 102(b) as being anticipated by Nakada (US Patent No. 5,961,578). Nakada'578 was cited for showing all the features of the present invention as claimed. Applicants strongly but respectfully traverse this rejection.

The present invention as now recited in claim 1 is directed to a tamper-resistant modular multiplication method for decreasing the relationship between data processing and consumption current therefor in an information-processing device which includes an input/output port communicating with an external device, a memory device for storing both programs and data, a central processing unit executing the data processing in accordance with the programs, and a bus connecting among the input/output port, the memory device and the central processing unit, when calculating a modular multiplication, A*B*R^(-1) mod N, which appears during performing crypto-processing as the data processing, the method comprising the steps of:

(1) selecting either of the following steps (2) and (3) at random;

(2) calculating S_1 = A*B*R^(-1) mod N where B is a multiplier, A is a multiplicand, N is a product of large primes, and R is 2^ (a bit length of a bit string of data) according to the Montgomery's method of calculating a modular multiplication for the data;

(3) calculating S_2 = {sN + A*(-1)^f}*{tN + B*(-1)^g}R^(-l) mod N, (among arbitrary integers s, t, f, g, at least one is an integer excepting 0, and f, g are both 0 or 1);

(4) repeating the above-mentioned steps (1), (2), (3) for each bit block consisting of the data, wherein finally when the step (2) is selected for a last bit block of the data, for a calculation result S_1, T_1 = S_1*R^(-1) mod N is calculated to output T_1, and when the step (3) is selected, for a calculation result S_2, T_2 = S_2*R^(-1) mod N is calculated to output N – T_2; and

(5) using T_1 and N - T_2 as a calculation result of a modular multiplication, A*B*R^ (-l) mod N.

The present invention as now recited in claim 5 is directed to a tamper-resistant modular multiplication method for decreasing the relationship between data processing and consumption current therefor in an information processing device which includes an input/output port communicating with an external device, a memory device for storing both programs and data, a central processing unit executing the data, processing in accordance with the programs, and a bus connecting among the input/output port, the memory device and the central processing unit, when calculating a modular multiplication, A*B mod p (p is a prime), which appears during performing crypto-processing as the data processing, the method comprising the steps of:

(1) selecting either of the following steps (2) and (3) at random;

(2) calculating S = A*B mod p where B is a multiplier, A is a multiplicand) for a bit string of data;

(3) calculating S = {Sp + A*(-l)^F)*{Tp + B*(-1)^G} mod p (among arbitrary integers s, t, f, g, at least one is an integer excepting 0, f and g are both 0 or 1, and f + g is an even number); and

(4) using the calculation result S which is selected from the step (2) or (3) as a calculation result of a modular multiplication, A*B mod p.

Further, the present invention as now recited in claim 9 is directed to a tamper-resistant modular multiplication method for decreasing the relationship between data processing and consumption current therefor in an information processing device which includes an input/output port communicating with an external device, a memory device for storing both programs and data, a central processing unit executing the data processing in accordance with the programs, and a bus connecting among the input/output port, the memory device and the central processing unit, when calculating a modular multiplication, A(x)*B(x) mod Φ(x), which appears during performing crypto-processing as the data processing, wherein Φ(x) is an irreducible polynomial of a variable x and the operation of coefficients of A(x)*B(x) is performed for modulus of a prime p which is 3 or more), the method comprising the steps of:

(1) selecting either of the following steps (2) and 3) at random

(2) calculating S(x) = A(x)*B(x) mod Φ(x), where A(x) or_B(x) is a polynomial of x;

(3) calculating S(x) = {sΦ(x) + A(x)*(-1)^f}*{tΦ(x) + B(x)*(-1)^g} mod Φ(x) (among arbitrary integers s, t, f, g, at least one is an integer excepting 0, f and g are both 0 or 1, and f + g is an even number); and

(4) using the calculation result S(x) which is selected from the step (2) and (3) as a calculation result of a modular multiplication, A(x)*B(x) mod Φ(x), for cryptoprocessing.

Among the main features of the present invention, claim 1 is directed to a method for decreasing the relationship between data processing and consumption current therefor in an information-processing device which includes an input/output port communicating with an external device, a memory device for storing both programs and data, a central processing unit executing the data processing in accordance with the programs, and a bus connecting among the input/output port, the memory device and the central processing unit, wherein one of two arithmetic expressions is selected for calculating a modular multiplication for each bit block consisting of a bit string of data. One expression is A*B*R^(-l) mod N, whereas another is an expression which leads to a calculation result reflecting the former expression. In the case where the latter expression is selected for the final bit block of the data, a little modification is required to the calculation result to obtain a correct one. The present claims 5 and 9 are similar to the claim 1, although the former expression is A*B mod p or A(x)*B(x) mod Φ(x) instead.

In contrast to the present invention, Nakada'578 is characterized by a microprocessor which realizes a fast power residue calculation "X^Y mod N"' (See col. 3, lines 49-50). Rather, Nakada'578 fails to provide any disclosure, teaching or suggestion related to the claimed features of the present invention so as to anticipate or even render obvious each and every feature of the invention. In particular, Nakada'578 fails to suggest any idea for addressing the type of attack where an attacker estimates what an information processing device executes by observing its consumption current. In the Office Action, the Examiner only pointed out that Nakada'578 discloses a method for sequentially calculating a modular multiplication, A*B*R^(-1) mod N, using a high speed calculation method.

Applicants will contend that the present invention as a whole is distinguishable and thereby allowable over the prior art.

Conclusion

In view of all the above, Applicant respectfully submits that certain clear and distinct differences as discussed exist between the present invention as now claimed and the prior art references upon which the rejections in the Office Action rely. These differences are more than sufficient that the present invention as now claimed would not have been anticipated nor rendered obvious given the prior art. Rather, the present invention as a whole is distinguishable, and thereby allowable over the prior art.

Favorable reconsideration of this application as amended is respectfully solicited. Should there be any outstanding issues requiring discussion that would further the prosecution and allowance of the above-captioned application, the Examiner is invited to contact the Applicant's undersigned representative at the address and phone number indicated below.

Respectfully submitted,

Stanley P. Fisher
Registration Number 24,344

Juan Carlos A. Marquez
Registration Number 34,072

REED SMITH LLP
3110 Fairview Park Drive
Suite 1400
Falls Church, Virginia 22042
(703) 641-4200

November 16, 2004

IN THE DRAWINGS

Please approve the changes to the drawings as outlined in the attached Letter to the Draftsperson, and as shown in the accompanying revised replacement drawings. Specifically, Figures 1 – 3 are being labeled as "PRIOR ART" in accordance with the Examiner's requirements.